T1078.004 Container Management- Unbounded Admin Access

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Who | Current text | Proposed text | Final text |
|  |  |  |  |  |
|  |  |  |  |  |

Description: An adversary may use a valid account with excessive privileges (i.e., does not follow least privilege policy) to gain access to container execution environment. If access rights are not tailored to specific needs of users, the risk to attack container execution increases.

Labelling:

* Sub-techniques: none
* Applicable Tactics: Initial-access, Privilege-Escalation, Defense-Evasion, Persistence
* Architecture Segment: Virtualization, OA&M
* Platform(s): Infrastructure, CI/CD & OA&M Tools
* Access type required: User/NPE/Administrative access
* Data Sources:
* Theoretical/Proof of concept/Observed: Observed

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| Specific example if known |  |

Mitigations

|  |  |
| --- | --- |
| **Name** | **Description** |
| M1032 | Use multi-factor authentication for cloud and virtualization OSS accounts used for VNF deployments, especially privileged accounts. |
| M1027 | Ensure that cloud accounts, particularly privileged accounts, have complex, unique passwords across all systems on the network. Passwords and access keys should be rotated regularly. This limits the amount of time credentials can be used to access resources if a credential is compromised without your knowledge. Rotate access keys regularly. |
| M1026 | Review privileged cloud account permission levels routinely to look for those that could allow an adversary to gain wide access. Unbound administrative access to accounts should be be discouraged when creating account policies. |
| M1018 | Periodically review user accounts and remove those that are inactive or unnecessary. Limit the ability for user accounts to create additional accounts. |
| M1017 | Applications may send push notifications to verify a login as a form of multi-factor authentication (MFA). Train users to only accept valid push notifications and to report suspicious push notifications. |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
|  |  |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| Containerized network functions | RAN and Core CNFs |
| Cloud/virtualized container Management controllers | Cloud, Kubernetes, or Openstack administrative controllers |

Detection

|  |  |
| --- | --- |
| **Name** | **Description** |
| DS0028 | Monitor for suspicious account behavior across cloud services that share account. Logon session logs and meta data helps determine if the session was an authorized activity. |
| DS0002 | Monitor user account authentication activity. Monitor the activity of cloud accounts to detect abnormal or malicious behavior, such as accessing information outside of the normal function of the account or account usage at atypical hours. Repeated attempts may be indictive of password guessing or brute force password cracking. Password policies supporting lockout requiring administrative reset may help. |
|  |  |

Post-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
|  |  |

References:

|  |  |
| --- | --- |
| Name | URL |
| ETSI NFV SEC023, Container Security Spec, section 5.4.4, Accessed 6/27/2022 | https://docbox.etsi.org/ISG/NFV/Open/Drafts/SEC023\_Container\_Security\_Spec/NFV-SEC023v005.zip |